

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.4806

(11/2017)

SERIES Y: GLOBAL INFORMATION
INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS,
NEXT-GENERATION NETWORKS, INTERNET OF
THINGS AND SMART CITIES

Internet of things and smart cities and communities –
Identification and security

Security capabilities supporting safety of the Internet of things

Recommendation ITU-T Y.4806

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

GLOBAL INFORMATION INFRASTRUCTURE

General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899

INTERNET PROTOCOL ASPECTS

General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999

NEXT GENERATION NETWORKS

Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999

FUTURE NETWORKS

Y.3000–Y.3499

CLOUD COMPUTING

Y.3500–Y.3999

INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES

General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	Y.4100–Y.4249
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	Y.4400–Y.4549
Services, applications, computation and data processing	Y.4550–Y.4699
Management, control and performance	Y.4700–Y.4799
Identification and security	Y.4800–Y.4899
Evaluation and assessment	Y.4900–Y.4999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Y.4806

Security capabilities supporting safety of the Internet of things

Summary

Recommendation ITU-T Y.4806 provides a classification of the security issues for the Internet of things (IoT) and examines how the security threats may affect safety, in order to determine which security capabilities specified in Recommendation ITU-T Y.4401/Y.2068 support safe execution of the Internet of things.

The appendices of this Recommendation consider how the joint analysis of threats and security capabilities mentioned herein may be used to establish security requirements for the different applications of the Internet of things.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.4806	2017-11-13	20	11.1002/1000/13391

Keywords

Internet of things, safety, security, security capability, security requirement, threat.

* To access the Recommendation, type the URL <http://handle.itu.int/> in the address field of your web browser, followed by the Recommendation's unique ID. For example, <http://handle.itu.int/11.1002/1000/11830-en>.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2018

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

	Page
1 Scope.....	1
2 References.....	1
3 Definitions	1
3.1 Terms defined elsewhere	1
3.2 Terms defined in this Recommendation.....	2
4 Abbreviations and acronyms	2
5 Conventions	3
6 Classification of security issues in the Internet of things by their impact vector	3
7 Security threats affecting safety in the Internet of things	6
7.1 Sources of security threats affecting safety	6
7.2 Scenarios of threatening functional safety	7
7.3 Requirement for the identification of security threats affecting safety	7
7.4 Safety measures and how they mitigate threats.....	7
7.5 Security measures	8
7.6 List of IoT security threats	8
8 Security capabilities for supporting safety in the Internet of things.....	10
8.1 Security capabilities initial list	10
8.2 Instantiation of security capabilities to address threats	11
Appendix I – Development of requirements according to identified threats.....	12
I.1 Smart traffic lights.....	12
I.2 Industrial control system	18
I.3 Smart wearable devices for industrial safety and productivity management.....	22
Bibliography.....	33

Downloaded from https://www.itu.int/ITU-T/ on 09/09/2017

Recommendation ITU-T Y.4806

Security capabilities supporting safety of the Internet of things

1 Scope

This Recommendation identifies security threats that may affect safety and security capabilities based on [ITU-T Y.4401].

Firstly, this Recommendation determines security threats with a possible impact on safety. Secondly, it identifies which security capabilities can be applied to mitigate these threats.

The Internet of things poses specific security challenges, which may not be covered by existing security objectives (such as confidentiality, integrity, availability) completely. Further elaboration of specific security countermeasures relies on an interpretation of security capabilities according to the identified threats.

This Recommendation is mostly applicable to safety-critical Internet of things (IoT) systems, such as industrial automation, automotive systems, transportation, smart cities, wearable and standalone medical devices, however it has no specific restrictions and may be used for any domain area of IoT.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

- | | |
|----------------|---|
| [ITU-T Y.4000] | Recommendation ITU-T Y.4000/Y.2060 (2012), <i>Overview of the Internet of things</i> . |
| [ITU-T Y.4100] | Recommendation ITU-T Y.4100/Y.2066 (2014), <i>Common requirements of the Internet of things</i> . |
| [ITU-T Y.4401] | Recommendation ITU-T Y.4401/Y.2068 (2015), <i>Functional framework and capabilities of the Internet of things</i> . |

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

- 3.1.1 adversary** [b-NISTIR 7298Rev2]: Individual, group, organization, or government that conducts or has the intent to conduct detrimental activities.
- 3.1.2 threat** [b-ISO/IEC 27000]: Potential cause of an unwanted incident, which may result in harm to a system or organization.
- 3.1.3 thing** [ITU-T Y.4000]: With regard to the Internet of things, this is an object of the physical world (physical things) or the information world (virtual things), which is capable of being identified and integrated into communication networks.

3.1.4 Internet of things (IoT) [ITU-T Y.4000]: A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.

NOTE 1 – Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.

NOTE 2 – From a broader perspective, the IoT can be perceived as a vision with technological and societal implications.

3.1.5 IoT actor [ITU-T Y.4100]: An entity that is external to the IoT and that interacts with the IoT.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 impact vector: A path comprised of the communication links by which an adversary, exploiting weaknesses of IoT services, platforms, or devices may have an effect on the virtual or physical thing.

3.2.2 virtual environment: An infrastructure comprised of virtual things and actors, which are capable of communicating with things in the Internet of things using the appropriate services and data.

3.2.3 physical environment: An infrastructure comprised of physical things and actors, which are capable of interacting with things in the Internet of things via their sensing and actuating mechanisms.

NOTE 1 – It depends on the context when the thing is considered as a part of the Internet of things and when it is a part of its virtual or physical environment. When the thing is in focus, all other things may comprise the environment.

NOTE 2 – Separation to the virtual and physical environment is made on a use-case basis. Some things may be conceived as a part of the virtual or physical environment according to the nature of its interaction with the thing in focus. For example, heating, ventilating and air conditioning (HVAC) systems are usually considered as a part of the physical environment because an effect of their work is physical. At the same time, there are known cases when a HVAC system remotely maintained by a contractor was used to penetrate the internal network. In this scenario, the HVAC system is considered as a part of virtual environment because its virtual interfaces are in focus.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AIC	Availability, Integrity, Confidentiality
CIA	Confidentiality, Integrity, Availability
HVAC	Heating, Ventilating and Air Conditioning
IT	Information Technology
IoT	Internet of Things
PPE	Personal Protective Equipment
SIS	Safety Instrumented System
XSS	Cross-Site Scripting

5 Conventions

None.

6 Classification of security issues in the Internet of things by their impact vector

Traditionally, security threats are considered as issues that arise in the virtual environment and target the data handling process. This leads to the interpretation of information technology (IT) security as the confidentiality, integrity, availability (CIA) set of aspects. Improper IT system behavior (e.g., software bugs, backdoors, Trojan programs) is also considered as a source of problems that affect these aspects and therefore cause only data handling concerns.

Attempts to classify security threats to the IoT in the same way they are classified for pure IT systems lead to difficulties in describing the potential physical impact caused by a cyberattack. One example of this approach is to rearrange the CIA triad to availability, integrity, confidentiality (AIC) by first ensuring the availability aspect in the physical systems and attaching less importance to confidentiality [b-NIST CPS]. The availability aspect is important, but alone, it cannot define all the physical characteristics that matter.

The Internet of things interconnects at least two types of environments: the virtual environment and the physical environment. Therefore, issues may arise from both types of environments and affect physical (P) aspects, virtual (V) aspects and the thing (T) itself. Figure 1 shows possible impact vectors in the Internet of things.

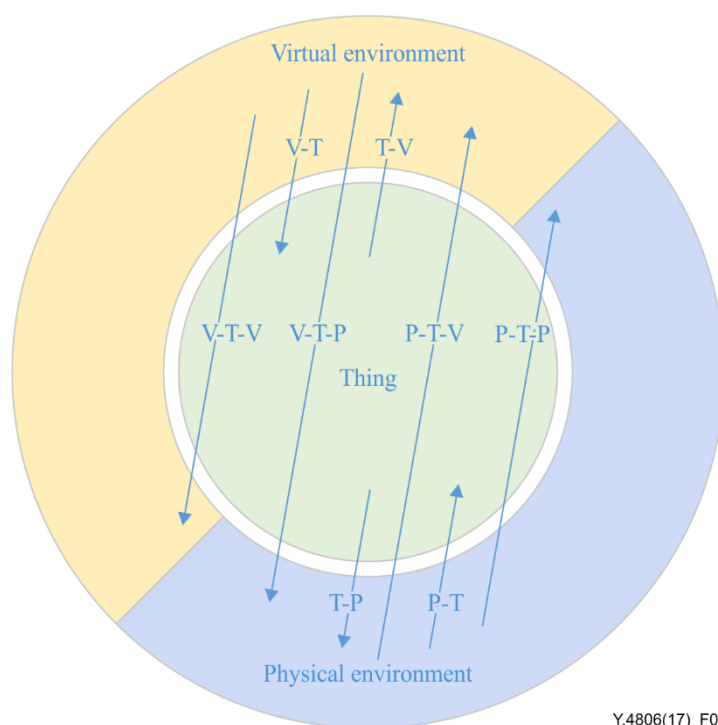


Figure 1 – Possible impact vectors in the Internet of things

The potential impact and prevention measures may vary significantly for these issues.

The classifications of security threats in the IoT domain are listed in Table 1, in accordance with the impact vectors shown in Figure 1.

The purpose of this classification is to determine which security threats are relevant to each impact vector according to the following criteria:

- They take place only for the physical things, that may be actuated by virtual means (i.e., things located in both environments), thus supporting the assumption about Internet of things as a key factor facilitating the issue.
- They may be enabled remotely, without getting physical or local access to the thing, thus providing the enhanced probability of such attacks in the connected world.
- Their impact may go beyond the confidentiality, integrity and availability of information, thus demonstrating the inability of many computer security methods to deal with them.

They may cause functional safety issues and thus provide a motivation to find ways to withstand them. This Recommendation will give further consideration to those threats that fit the criteria listed above.

Table 1 – Classification of computer security threats in the Internet of things according to their impact vector

Impact vector	May take place only for the things presented both in the virtual and physical environment	May be caused remotely without physical access to the thing	May go beyond the aspects from the CIA triad	May cause functional safety issues	Description	Examples
V-T	No	Yes	No	No	An attack targeting the thing from within its virtual environment	Denial of service attack Confidential information stealing
T-V	No	Yes	No	No	Exploiting software bugs or concealed features harming security of environment without any influence. May be treated as an informational safety issue.	Improperly implemented or infected with malware virtual thing capable of harming other
V-T-V	No	Yes	No	No	An attack targeting the virtual environment of the thing by exploiting its improperly implemented features	Cross-site scripting (XSS) Distributed denial of a service using botnet
V-T-P	Yes	Yes	Yes	Yes	An attack targeting the physical environment of the thing(s) and intended to cause physical damage or harm physical aspects of its functioning.	Attack on a smart vehicle intended to change its driving direction, speed, or cause any other physical effect Attack on industrial control system affecting the execution or efficiency of the technological

Table 1 – Classification of computer security threats in the Internet of things according to their impact vector

Impact vector	May take place only for the things presented both in the virtual and physical environment	May be caused remotely without physical access to the thing	May go beyond the aspects from the CIA triad	May cause functional safety issues	Description	Examples
						process Attack on the wearable medical device in order to change the taken dose of medicines
P-T-V	Yes	No	No	No	Actions posing problems for information security aspects by purely physical means.	Destroying hardware, cable breakage Physical tampering of video surveillance systems by placing a picture in front of a camera
P-T-P	No	No	Yes	Yes	Physical hazards that are usually capable of harming the physical environment or people.	Sabotage, negligence Faulty treatment
T-P	No	No	Yes	Yes	Software bugs or functions that may affect important factors in the physical environment. May be treated as thing functional safety.	System functions implemented without or with insufficient consideration of safety requirements
P-T	No	No	Yes	Yes	Physical hazards that are usually capable of harming the system or its components.	Disregard of operating instructions Faulty treatment

The vectors that arise from the virtual environment are cyberattacks. Cyberattacks may be performed remotely without getting physical access. The vectors V-T and V-T-V are generally well studied within the traditional computer and network security area. These vectors are not addressed in detail in this Recommendation.

However, the vector V-T-P targeting the physical environment is not well studied yet.

All issues that have their roots in the thing behavior due to its improper implementation or due to being compromised may be interpreted as pure safety problems in the informational and functional

aspect (vectors T-V and T-P respectively). These vectors are addressed in detail in this Recommendation.

The vectors P-T-P and P-T that arise in the physical environment are actually among those that are usually capable of harming the thing and surrounding infrastructure. These hazards are usually mitigated by a set of physical, organizational and deterrent measures. These vectors are not addressed in detail in this Recommendation.

The vector P-T-V refers to the effects on information security by purely physical means. Although such attacks may be important, they are specific to the IoT domain or environment of the thing. This vector is not addressed in detail in this Recommendation.

All threats targeting virtual environment may be mapped onto the CIA triad to determine the security objectives and appropriate security measures that need to be implemented to withstand attacks. At the same time, factors which may jeopardize the physical process, or harm the environment, or even human health and life may be hard to interpret in terms of confidentiality, integrity or availability of information.

Based on these possible types of issues in the IoT, it is necessary to pay special attention to the V-T-P impact vector, to reveal the conditions under which the existing methods of ensuring proper thing behavior may be ineffective for this impact and to propose an appropriate approach to threat modeling that eliminates the relevant safety risks.

It is worth mentioning that the impact vector may be interpreted as V-T-P even if the result of attack is data alteration only, but where the physical objects are finally damaged because of wrong decisions or actions according to these data. An example could be an aircraft crash caused by wrong data about the altitude in poor visibility and rough weather conditions.

This Recommendation will focus on the analysis of threats and measures associated with the V-T-P impact vector.

While the methods that guarantee safe things behavior in some IoT domains are well known and have been applied for decades, these methods may not always give the same guarantees in the event of deliberate attempts to cause improper thing behavior. The IoT has a wide-ranging potential for the implementation of such attempts due to the provided communication capabilities.

7 Security threats affecting safety in the Internet of things

Security threats affecting safety generally use the V-T-P impact vector to affect the physical environment (in particular, to cause a safety violation) by exploiting thing features or vulnerabilities.

7.1 Sources of security threats affecting safety

The sources of security threats affecting safety lie in the virtual environment. These sources may pose risks for both unintentional mistakes and deliberate abuses of thing functionality.

The set of potential malicious actors formally includes any actor that may access the thing by any virtual means. An external attacker remotely accessing the system is usually considered as a striking example for demonstration purposes. In fact, any IoT actor both in the virtual and physical environment may be considered as a possible source of issues, or as an adversary.

Further restrictions on the list of possibly malicious actors are set according to the assumptions about their trustworthiness. The role of assumptions is explained in more detail in clause 7.3.

Thus, the sources of attacks from within a virtual environment in the IoT are indistinguishable from the sources of attacks on the security of pure IT systems. Those of sources that may affect the physical environment are of the particular interest for this Recommendation.

7.2 Scenarios of threatening functional safety

For different IoT domains, the ways in which the physical aspects of thing functioning are impacted will obviously vary. It is worth mentioning that if the physical process is directly controlled by commands issued by a virtual thing; these commands are usually checked to avoid direct harm. Hence, scenarios, whereby safety is affected by virtual means, have to be more sophisticated. For example, an adversary may use two independent channels to cause an undesirable effect (e.g., one for disabling the protection mechanisms and another for placing the thing into an invalid state).

7.3 Requirement for the identification of security threats affecting safety

An effective threat modelling technique takes into account both possible system flaws and threats that may be of interest to the adversary. Threat identification and modelling is used to find out which vulnerabilities of the thing are most dangerous and how they can be exploited by the adversary to violate the security aspects and cause harm (in particular to safety).

The validity of the results of threat identification depends on the correctness of the assumptions set out. This is true both for information security and for functional safety. In particular, if safety mechanisms rely on assumedly reasonable actor behavior (even taking into account unintentional mistakes), a safety violation may be caused by an intentionally malicious actor. Security incidents also often happen according to an unforeseen system usage scenario. The adversary breaks the assumptions made during threat modelling and security mechanism implementation to bypass this mechanism.

Identification of security threats affecting safety requires:

- The revision of assumptions made by safety engineers from a security point of view.
- Consideration of possible weaknesses in the protection components.
- Using an approach allowing the unification of security threats and safety hazards within a structured (possibly formal) description.

7.4 Safety measures and how they mitigate threats

Though safety requirements posed by the things across IoT domains can vary drastically, generally safety provisions for diverse applications include monitoring and enforcement mechanisms. This simple classification also covers the extreme cases. If the safety mechanism is oriented more on placing the thing in a safe state, the monitoring just ensures that the condition to enforce protection is fulfilled. If the interference into the process is undesirable or unreasonable, the monitoring may be the only mechanism that follows up on the safety parameters.

In some cases, the V-T-P impact vector can be effectively eliminated by safety enforcement measures that were initially designed for the T-P vector; but in other cases, this will not be possible. The analysis of such other cases reveals the following reasons for this ineffectiveness:

- **Possibility of tampering or bypassing the safety restrictions.** Safety measures usually do not seek to cover the possibility of intentional violations. The violations they address are considered as accidents or sets of coincidences.
Exploitation of the weaknesses of safety mechanisms helps to make the adversary's actions appear safe when they are not. For this purpose, the adversary injects the specifically formed data as the system input to mislead the validation algorithms.
- **Attacks on separately implemented safety mechanisms.** Implementation of safety mechanisms by an independent party and installation separately from the controlled system reduce this risk of common cause failures. At the same time, the adversary may compromise standalone safety monitoring and enforcement mechanisms if they are not properly protected.